

**Implementation Guide:  
Lacework Cloud Security Platform with AWS Control  
Tower**



# Table of Contents

Foreword	3
Solution Overview and Features	4
Audit Your AWS Configuration	4
Actionable Auditing of S3 Bucket Security Configuration	4
Ongoing Monitoring of Activity	4
Shift-Left DevSecOps	5
Cloud Native Runtime Workload Protection	5
The Power of Polygraph	5
Architecture Diagram	6
Setup Flow	7
New Account Flow	7
Prerequisites	8
Deployment and Configuration Steps	8
Best Practices	14
Lacework API Keys	14
Estimated Pricing	14
FAQs	14
Additional resources	14
Partner Contact Information	14

## Foreword

The Lacework Cloud Security Platform delivers comprehensive and continuous end-to-end AWS security and configuration support for both workloads and accounts running in Amazon cloud environments. As more organizations move their critical workloads to the cloud, there is an increasing need for a single, unified solution like the Lacework Cloud Security Platform that can identify, analyze, and report on misconfigurations, vulnerabilities, and behavioral anomalies in user and account behavior.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure the Lacework Cloud Security Platform in AWS Control Tower environments while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

## Solution Overview and Features

AWS users understand the shared responsibility concept of cloud security, but also recognize that effective security demands more than just operating off of signatures and custom rules. Every activity within a cloud environment increases the potential for threats, and AWS users must have a solution that not only identifies changes, but understands the security context of them. To address the agile nature of the cloud, Lacework provides comprehensive, continuous end-to-end security and configuration support for workloads and accounts running in AWS environments. The following sections highlight the features of the Lacework Cloud Security Platform.

### Audit Your AWS Configuration

- Find Identity and Access Management (IAM) vulnerabilities, including the use of “root” account, password requirements, and use of multi-factor authentication.
- Check for logging best practices, ensure AWS CloudTrail is enabled across regions, and log files validated and encrypted.
- Monitor critical account activity such as unauthorized API calls and use of the management console and the “root” account.
- Confirm secure network configurations, including limiting access to vulnerable ports, enforcing “least access” privileges and checking for the use of flow logging.
- Assess your S3 settings for S3 buckets at risk.

### Actionable Auditing of S3 Bucket Security Configuration

- Find potentially exposed AWS S3 buckets configured for external access.
- Identify buckets out of compliance with the CIS Benchmark for AWS.
- Use of encryption at rest and in transit.
- Only users with multi-factor authentication can delete buckets.
- Versioning to protect against deletion or overwrite.
- Get specific recommendations on how to fix violations.

### Ongoing Monitoring of Activity

- Activity on AWS resources, such as new activity in a region, activation of new AWS services, or changes to access control lists.
- Changes to users, roles, or access policies. Access or customer master key tampering.

- Reduce alert fatigue with customizable alerts and reports that eliminate repetitive or irrelevant results.

## Shift-Left DevSecOps

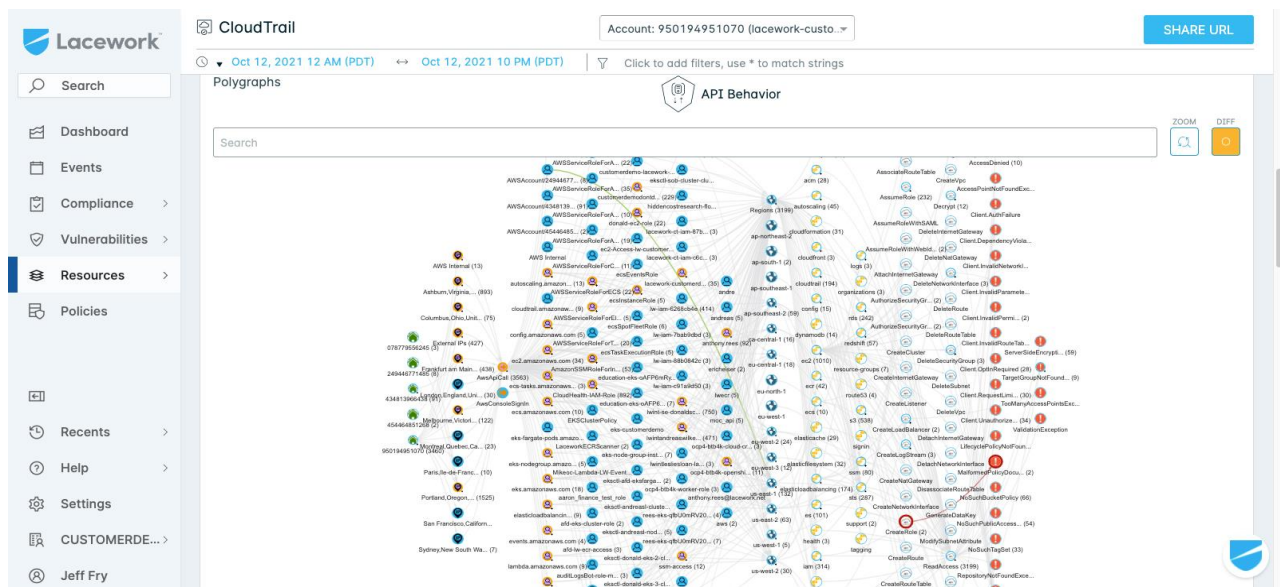
- Incorporate software vulnerability detection in your AWS CodePipeline and CodeBuild steps to secure your software delivery pipeline.
- Scan your Amazon ECR registries for image vulnerabilities.

## Cloud Native Runtime Workload Protection

- Actively monitor your Amazon EC2 hosts for vulnerabilities and intrusions.
- Identify runtime container vulnerabilities and anomalous behavior in Amazon ECS and EKS environments.

## The Power of Polygraph

Our foundation is based on the patent-pending Polygraph technology, a context-rich baseline built from collecting high-fidelity machine, process, and user interactions over time. This technology dynamically develops a behavioral and communication model of your services and infrastructure that understands natural hierarchies (processes, containers, pods, machines, etc.) and aggregates them to develop behavioral models at scale. Together with a behavioral model, the Polygraph is able to monitor your infrastructure for activities that fall outside the model and dynamically update as behaviors change over time.



Using this information, the Polygraph detects anomalies and generates high-fidelity alerts appropriate to your unique environment. Polygraph maps the truth of your cloud instance and helps users quickly visualize

the 'who, what, where, and how far' of an event, speed investigation, and triage issues saving organizations time and money.

Lacework Polygraph uses deviation from a temporal baseline to detect deviations or changes in the behavior resulting in meaningful alerts. Alerts are either due to a desired change, misconfiguration, or malicious activity. The Lacework Polygraph then scores the alerts based on severity and threat.

Lacework Polygraph breach detection is more precise and accurate because of key technology innovations:

- Capturing behavior at process/container-level
- Separating interactive and non-interactive traffic
- Alert generation at the analysis group-level
- Advanced deductive analysis that does not rely on heuristics

## Architecture diagram

Lacework's AWS Control Tower integration enables a seamless AWS account onboarding experience with the Lacework Cloud Security Platform. Account administrators can automatically add Lacework's security auditing and monitoring to new AWS accounts during account creation. All the required Lacework and AWS account configurations that allow access to AWS configuration and CloudTrail logs are managed for you by Lacework's AWS Control Tower integration.

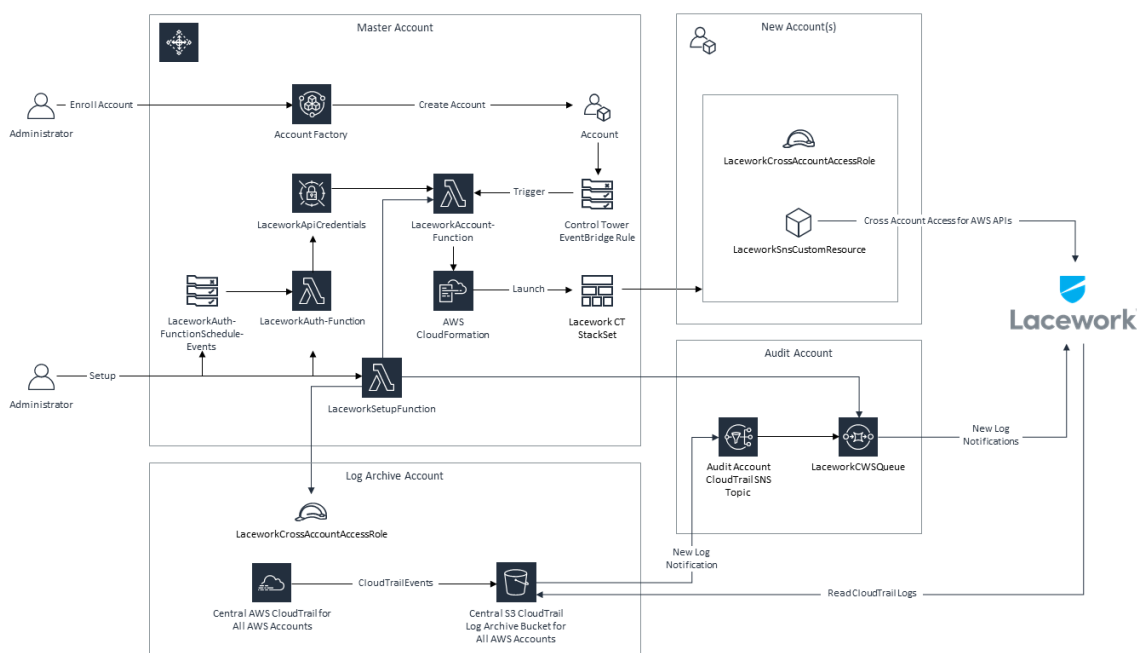


Figure 1 Lacework's Control Tower Integration Architecture Diagram

## Setup Flow

1. The Administrator applies Lacework's main Control Tower Integration template in CloudFormation for the initial setup.
2. This template provisions all resources which includes a stack set, roles & permissions, Lambda functions, SQS queues and EventBridge rule.
3. Via LaceworkSetupFunction Lambda, a new cross-account role is set up in the Log Archive account and a new SQS queue is set up in the Audit account. The SQS queue allows Lacework to receive notifications of new audit logs in S3 from the centralized CloudTrail that collects activity from all accounts. Lacework processes these logs for behavior analysis for all AWS accounts.
4. The LaceworkSetupFunction acquires the initial Lacework access token.
5. The LaceworkSetupFunction provisions any existing ACTIVE AWS accounts by sending an SNS message to the StackSet Lambda Function if specified with the **Monitor Existing Accounts** option.
6. The LaceworkAccountFunction Lambda creates a new Stack instance(s) for the account(s).
7. The Stack instance creates a new cross-account role and allows Lacework to monitor the account via AWS APIs.
8. The Stack instance notifies Lacework of the new account through an SNS custom resource notification, LaceworkSNSCustomResource. The account is created in Lacework.
9. A scheduled event rule periodically triggers the LaceworkAuthFunction Lambda to acquire a temporary access token from Lacework.

## New Account Flow

1. A new AWS account triggers a Control Tower lifecycle event which is picked up by the EventBridge rule.
2. The EventBridge rule triggers the LaceworkAccountFunction Lambda to create a new Stack instance for the account.
3. The LaceworkAccountFunction Lambda creates a new Stack instance(s) for the account(s).
4. The Stack instance creates a new cross-account role and allows Lacework to monitor the account via AWS APIs.
5. The Stack instance notifies Lacework of the new account through an SNS custom resource notification, LaceworkSNSCustomResource. This sends an SNS notification to Lacework and the account is created in Lacework's platform.

## Prerequisites

If you are new to AWS, see [Getting Started with AWS](#)

For [additional information](#) on AWS Marketplace

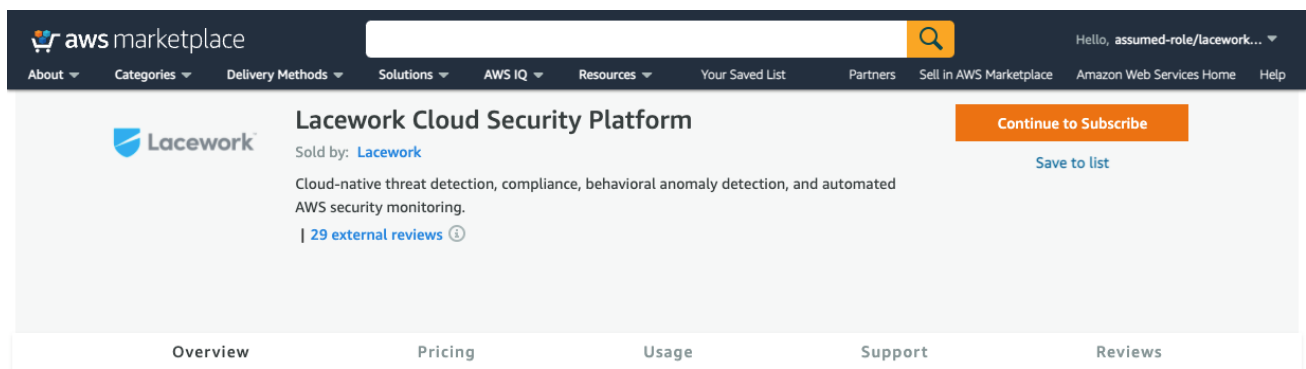
To get started with AWS Control Tower, check out the [Control Tower User Guide](#)

## Deployment and Configuration Steps

The following steps will set up Lacework's AWS Control Tower integration to monitor existing ACTIVE AWS accounts if specified and new enrolled AWS accounts.

### Step 1.1: Subscribe to Lacework Cloud Security Platform on AWS Marketplace.

Locate the **Lacework Cloud Security Platform** in the [AWS Marketplace](#).



The screenshot shows the AWS Marketplace product page for Lacework Cloud Security Platform. The page header includes the AWS Marketplace logo, a search bar, and a user profile dropdown. The main content area features the Lacework logo, the product name "Lacework Cloud Security Platform", and a "Continue to Subscribe" button. Below the product name, it states "Sold by: Lacework" and provides a brief description: "Cloud-native threat detection, compliance, behavioral anomaly detection, and automated AWS security monitoring." There is also a link to "29 external reviews". At the bottom of the product card, there are tabs for "Overview", "Pricing", "Usage", "Support", and "Reviews".

### Product Overview

Lacework delivers complete security and compliance for the cloud.

While the cloud enables enterprises to automatically scale workloads, deploy faster, and build freely, it also makes it increasingly difficult to: maintain visibility, remain compliant, stay free from known vulnerabilities, and track activity in both host workloads and ephemeral infrastructure within their environments.

The Lacework Cloud Security Platform is cloud-native and offered as-a-Service; delivering continuous build to run-time threat detection, behavioral anomaly detection, and compliance across multi-cloud environments, workloads, accounts, containers, and Kubernetes. This single platform solution helps businesses (DevOps and IT Security teams) develop at lightning speed, while staying safe during both build-time and run-time in their efforts to shift left. Customers are able to significantly drive down costs and risk by freeing themselves from the burden of unnecessary hardware or software maintenance, manual rule configuration, and excessive alerting.

### Highlights

- Threat Detection, Compliance, and Automated AWS Security Monitoring.  
<https://www.lacework.com/aws-security/>
- Actionable auditing of security configurations, ongoing monitoring of user activity with behavioral detection, automated & scalable architecture with no added complexity or performance penalties all while helping meet your AWS compliance mandates.
- Lacework creates a temporal baseline built from collecting detailed machine/process/users interactions, then uses this to detect anomalies, generate appropriate alerts, and provide details for

Select **Continue to Subscribe** button.

**Continue to Subscribe**

## Step 1.2: Contract Duration and Renewal

On the next screen, you can configure your contract. You can select the **Contract Duration** and set the **Renewal Settings**.

The screenshot shows the 'Configure your Software Contract' page for the 'Lacework Cloud Security Platform'. The page is part of the AWS Marketplace interface, with a navigation bar at the top containing 'About', 'Categories', 'Delivery Methods', 'Solutions', 'AWS IQ', 'Resources', 'Your Saved List', 'Partners', 'Sell in AWS Marketplace', 'Amazon Web Services Home', and 'Help'. A search bar and a user profile 'Hello, assumed-role/lacework...' are also visible.

The main content area is titled 'Configure your Software Contract' and includes the following sections:

- How long do you want your contract to run?**: Three radio button options: '12 months' (selected), '24 months', and '36 months'.
- Renewal Settings**: A section titled 'Auto Renew when this contract ends on - Wed Oct 12 2022?' with 'Yes' selected. Below it, a disclaimer states: 'I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.'
- Create contract**: A button at the top right of the main content area.
- Terms and Conditions**: A text block stating: 'By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services'.
- Total Contract Price**: A summary box showing '\$0' for 'Due Today' and 'Auto Renew -Yes'.
- Select contract Option(s)**: A red text prompt at the bottom right.

## Step 1.3: Select Contract Options

Select the Contract Options to be activated with your contract.

The screenshot shows the 'Select Contract Options' page for the 'Lacework Cloud Security Platform'. The page is part of the AWS Marketplace interface, with a navigation bar at the top containing 'About', 'Categories', 'Delivery Methods', 'Solutions', 'AWS IQ', 'Resources', 'Your Saved List', 'Partners', 'Sell in AWS Marketplace', 'Amazon Web Services Home', and 'Help'. A search bar and a user profile 'Hello, assumed-role/lacework...' are also visible.

The main content area is titled 'Select Contract Options' and includes the following sections:

- Renewal Settings**: A section titled 'Auto Renew when this contract ends on - Wed Oct 12 2022?' with 'Yes' selected. Below it, a disclaimer states: 'I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.'
- Contract Options**: A section containing a table of options:

Standard Cloud Security	\$5000 / Units	<input type="text"/>
-------------------------	----------------	----------------------

Per Cloud Account. Agentless. Unit=200 Cloud Assets (EC2, RDS, ELB, +)
- Terms and Conditions**: A text block stating: 'services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services'.
- Total Contract Price**: A summary box showing '\$0' for 'Due Today' and 'Auto Renew -Yes'.
- Select contract Option(s)**: A red text prompt at the bottom right.

Below the 'Contract Options' section, there is a disclaimer: 'You may increase your contract at any time. Changes will be billed on a pro-rated basis. If you have opted in for automatic renewal, your contracts will automatically renew at the end of each term until you change your automatic renewal selection.'

### Step 1.4: Create the Contract and Pay

Once you have configured your contract, you can click on the Create contract button.

[Create contract](#)

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services

<b>Total Contract Price</b>	<b>\$5000.00</b>
<small>Due Today Auto Renew -Yes</small>	
Standard Cloud Security X 1 Units	\$5000.00

You will be prompted to confirm the contract. If you agree to the pricing, select the **Pay Now** button.

### Step 1.5: Register with Lacework

1. On the next page, register with Lacework to create your new Lacework account.
2. Lacework will send a confirmation email after completing your registration.



#### One more step...

Thank you for your purchase of **Lacework Cloud Security Platform**. Complete your registration now to activate your subscription. The purchase is not complete until this form has been submitted.

Full Name \*

Email Address \*

Company \*

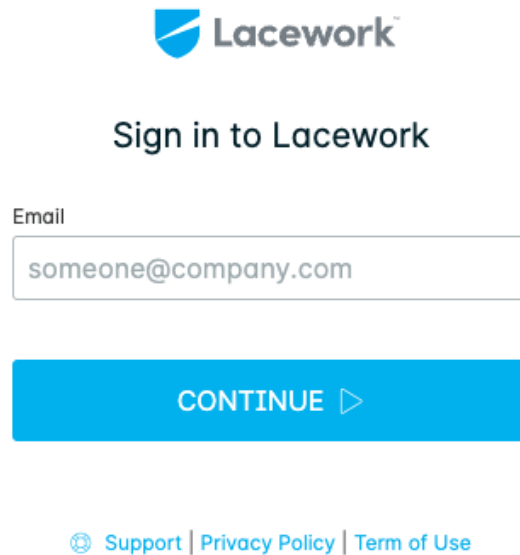
Additional Note

[COMPLETE REGISTRATION](#)

By submitting this form, I agree that my information will be shared with Lacework and Tackle.io in accordance with the [Privacy Policy](#)

## Step 1.6: Log into the Lacework Cloud Security Platform Console

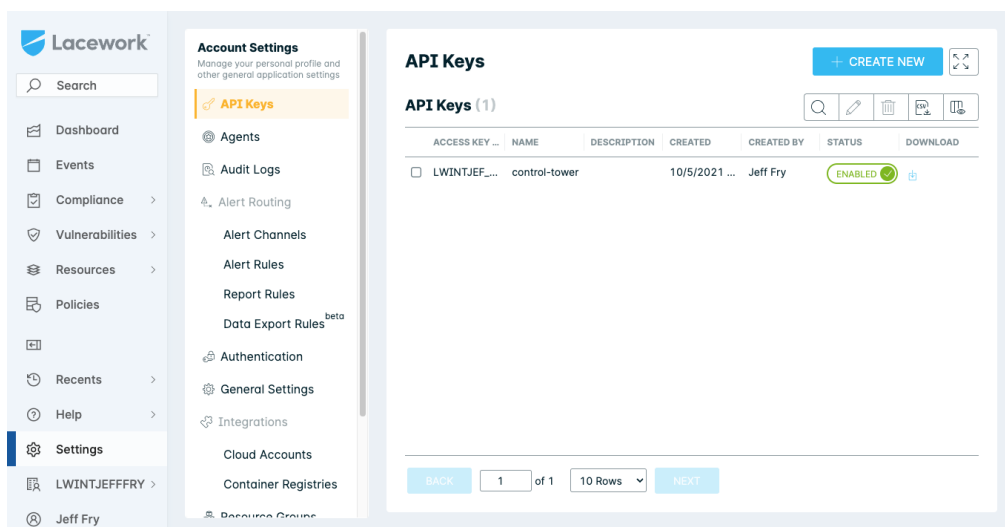
From your confirmation email, use the login link to access your console with your email address.



The image shows the Lacework login page. At the top is the Lacework logo. Below it is the heading "Sign in to Lacework". There is an "Email" label above a text input field containing "someone@company.com". Below the input field is a large blue button with the text "CONTINUE" and a right-pointing triangle. At the bottom of the page are three links: "Support", "Privacy Policy", and "Term of Use", each preceded by a small globe icon.

## Step 1.7: Generate a Lacework API Access Key

1. In your console, go to **Settings > API Keys**.
2. Click on the **Create New** button in the upper right to create a new API key.
3. Provide a name and description and click **Save**.
4. Click the download button to download your API keys.
5. Copy the **keyId** and **secret** from this JSON file.



The screenshot shows the Lacework console interface. On the left is a navigation sidebar with the Lacework logo and a search bar. Below the search bar are menu items: Dashboard, Events, Compliance, Vulnerabilities, Resources, Policies, Recents, Help, and Settings (which is highlighted). Under Settings, there are sub-items: LWINTJEFFRY and Jeff Fry. The main content area is titled "API Keys" and has a "+ CREATE NEW" button in the top right. Below the title is a table with the following columns: ACCESS KEY, NAME, DESCRIPTION, CREATED, CREATED BY, STATUS, and DOWNLOAD. The table contains one row with the following data: [checkbox], LWINTJEF..., control-tower, 10/5/2021 ..., Jeff Fry, ENABLED (with a green checkmark), and a download icon. At the bottom of the table are pagination controls: "BACK", "1" of 1, "10 Rows" (with a dropdown arrow), and "NEXT".

## Step 1.8: Login into your AWS Master Account

1. Login in to AWS master account with Administrator permissions.
2. Select the AWS region where your AWS Control Tower is deployed.

## Step 1.9: Deploy the Lacework AWS Control Tower Integration with CloudFormation

1. Follow this link to go to your CloudFormation console.



2. For most deployments, the **Basic Configuration** parameters are all that are required. Use the **Advanced Configuration** for customization.

Stack name  
lct-1020-2135  
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**  
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Basic Configuration**

**Lacework Account Name**  
Your Lacework account name. i.e. <account name>.lacework.net  
lwintjeffry

**Lacework Access Key ID**  
Lacework API Secret Key ID. See <https://support.lacework.com/hc/en-us/articles/360011403853-Generate-API-Access-Keys-and-Tokens>  
\*\*\*\*\*

**Lacework Secret Key**  
Lacework API Secret Key. See <https://support.lacework.com/hc/en-us/articles/360011403853-Generate-API-Access-Keys-and-Tokens>  
\*\*\*\*\*

**StackSet Name**  
The name for the Lacework Control Tower StackSet  
Lacework-CT

**Capability Type**  
The Lacework Control Tower StackSet type to use  
CloudTrail+Config

**Monitor Existing Accounts**  
Choose to monitor any existing accounts. SUSPENDED accounts are skipped.  
Yes

**KMS Key Identifier ARN for CloudTrail S3 Logs Decrypt**  
Provide the ARN of the KMS key for decrypting S3 log files decryption if necessary. Won't use KMS decrypt if no key provided.

**Log Account Name**  
Your AWS Control Tower log account name.  
Log Archive

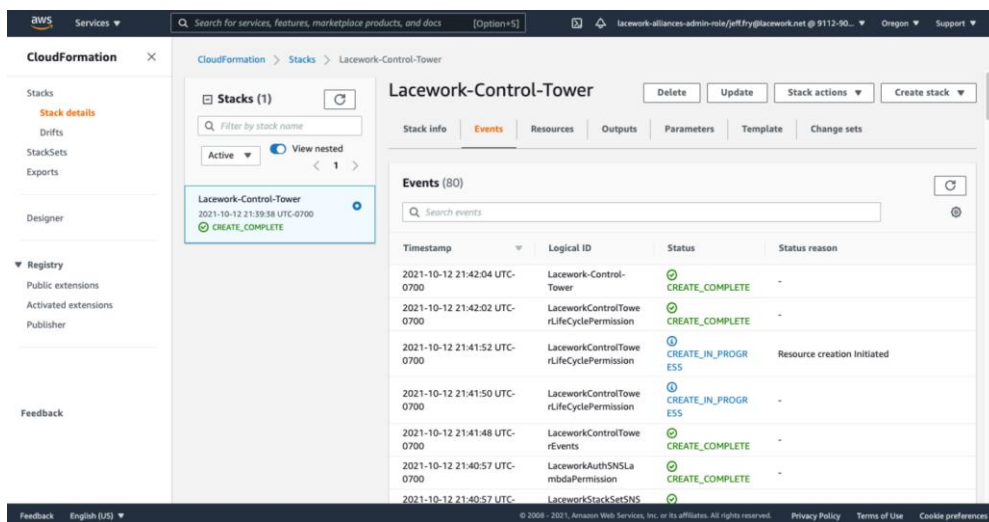
**Audit Account Name**  
Your AWS Control Tower audit account name.  
Audit

3. Enter a **Stack name** for the stack.
4. Enter your **Lacework Account Name**.
5. Enter your **Lacework Access Key ID** and **Secret Key** that you copied from your previous API Keys JSON file.
6. For **Capability Type**, the recommendation is to use **CloudTrail+Config** for the best capabilities.

7. Choose whether you want to **Monitor Existing Accounts**. This will set up monitoring of ACTIVE existing AWS accounts.
8. If your CloudTrail S3 logs are encrypted, specify the KMS Key Identifier ARN.
9. Updated the Control Tower **Log Account Name** and **Audit Account Name** if necessary.
10. Accept the AWS CloudFormation terms and click **Create stack**.

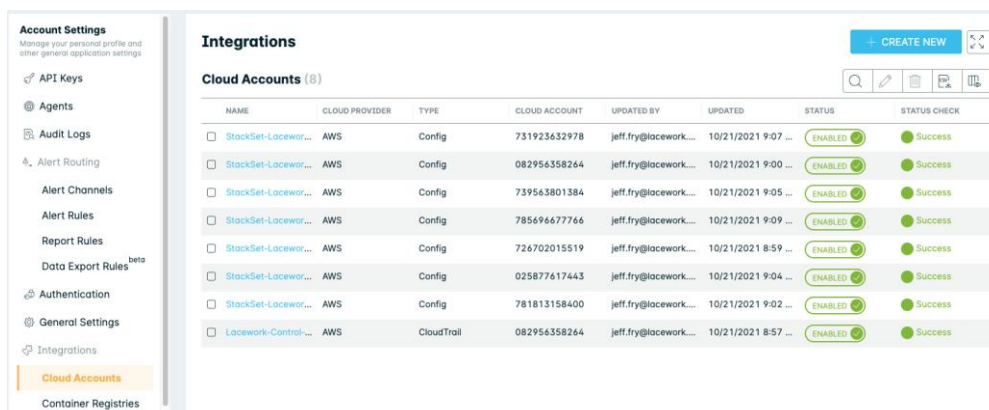
## Step 2.0: CloudFormation Progress

1. Monitor the progress of the CloudFormation deployment. It will take several minutes for the stack to create the resources that enable the Lacework Control Tower Integration.
2. When successfully completed, the stack shows CREATE\_COMPLETE.



## Step 2.1: Validate the Lacework Control Tower Integration

1. Login to your Lacework Cloud Security Platform console.
2. Go to **Settings > Cloud Accounts**.
3. You should see a list of AWS accounts that are now being monitored by Lacework. The Cloud Account column values correspond to the AWS Account IDs.



## Best Practices

### Lacework API Keys

The Lacework API keys JSON file should be stored in a secure place. If these API keys need to be changed, they are stored using AWS Secrets Manager under the name LaceworkApiCredentials. If needed, you can update these keyId and secrets values in AWS Secrets Manager.

## Estimated Pricing

The Lacework Cloud Security Platform purchased through the AWS Marketplace provides flat pricing based on the number of units where a unit is 200 cloud assets (EC2, RDS, ELB, etc.) being monitored. This pricing is offered in terms of 12, 24 and 36 months. Pricing is listed [here](#) in the AWS Marketplace.

## FAQs

Lacework FAQs can be found online [here](#).

## Additional resources

[Getting Started](#)

[Administration](#)

Additional Lacework documentation can be found online [here](#).

## Partner Contact Information

Lacework customers can submit a support request through their support portal [here](#). Otherwise, send a request [here](#).